Live Hacking & Cybersecurity

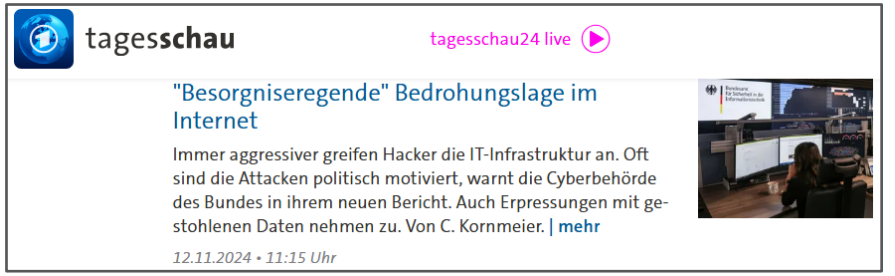
Bremen, 08.10.2025

CLA Global

INDEPENDENT NETWORK MEMBER

Aktuelle Bedrohungslage & Angriffsszenarien

- Zahl der Cyberangriffe steigt weiter rasant –
  betroffen sind Unternehmen jeder Größe und Branche
  - Ø 309.000 neue Schadprogramm-Varianten pro Tag / Steigerung: ca. 26 %
    (lt. BSI – Die Lage der IT- Sicherheit in Deutschland 2024)
  - Rund 333.000 in Deutschland gemeldete Cybercrime-Fälle in 2024,
    davon ca. 131.000 in Deutschland und ca. 202.000 aus dem Ausland verübt
    (lt. BKA - Bundeslagebilds Cybercrime 2024)
  - Wirtschaftlicher Schaden 2024 durch Cyberattacken in Deutschland:
    ca. 179 Milliarden Euro (lt. Bitkom e. V.)
- Besonders im Fokus:
  - DoS und DDoS-Angriffe
  - Malware / Ransomware
  - Phishing & Deepfakes (zunehmend KI-gestützt)
  - Identitätsdiebstahl (zunehmend KI-gestützt)
  - Automatisierte und dateilose Angriffe


tagesschau

tagesschau24 live

"Besorgniseregende" Bedrohungslage im Internet

Immer aggressiver greifen Hacker die IT-Infrastruktur an. Oft sind die Attacken politisch motiviert, warnt die Cyberbehörde des Bundes in ihrem neuen Bericht. Auch Erpressungen mit gestohlenen Daten nehmen zu. Von C. Kornmeier. | mehr

12.11.2024 • 11:15 Uhr


Bild

STARTSEITE NEWS POLITIK REGIO UNTERHALTUNG KAUFBERATER SPORT FUSSBALL RATGEBER GESUNDHEIT SEX & LIEBE AUTO SPIELE

Hauptstadt-Flughafen im „Ausnahmemodus“

Problem-BER

Nach Cyberangriff: Auch heute drei Flüge abgesagt +++ Gepäckabfertigung funktioniert weiterhin nicht


zdfheute

Cybersicherheit: Rekordschaden durch Spionage und Hacker

Bitkom-Studie in Deutschland

Rekordschaden durch Spionage und Hacker

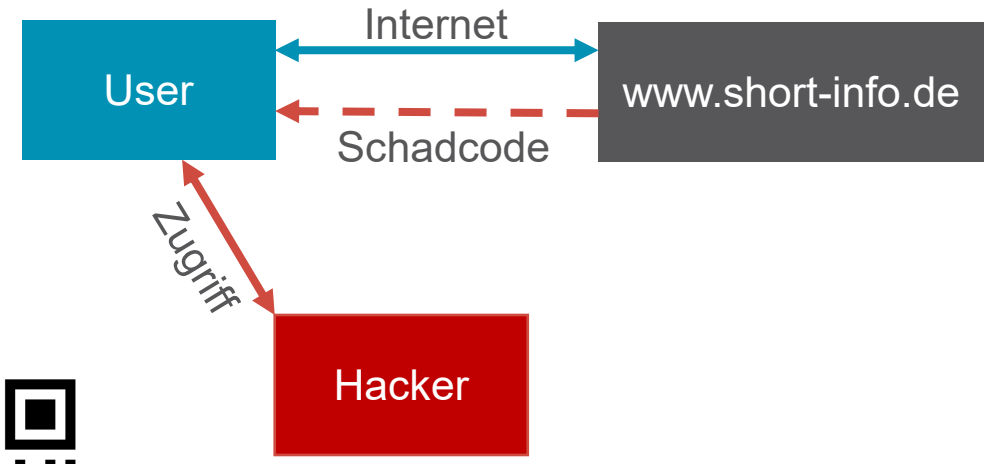
18.09.2025 | 10:44

Cyberangriffe verursachen Rekordschäden für deutsche Firmen. Immer mehr Attacken seien auf Angreifer aus Russland und China zurückzuführen, heißt es in einer neuen Studie.

Live-Hacking zum Mitmachen garantiert ohne „Nebenwirkungen“

Besuchen Sie doch bitte einmal die Web-Seite: www.short-info.de

Szenario-Beschreibung:



Prävention & Handlungsempfehlungen - Regeln für den Schutz vor Phishing-Mails

Identifikation:
BSI empfiehlt 3-Sekunden-Sicherheits-Check

1. Ist die Absenderadresse bekannt? Weist diese Ungereimtheiten auf (z.B. Domänenname etc.)
2. Ist der Betreff sinnvoll? (oft vage formuliert "Ihre Rechnung“, „Mahnung“)
3. Wird ein Anhang von diesem Absender erwartet?

weitere Indikatoren:

4. Unpersönliche Anrede, evtl. schlechtes Deutsch / Sonderzeichen (werden immer besser)
5. Dringender Handlungsbedarf (Druck bzw. Drohungen)
6. Abfrage vertraulicher Daten (IDs, Passwörter)
7. Links und URLs (Mouseover) stimmen nicht überein

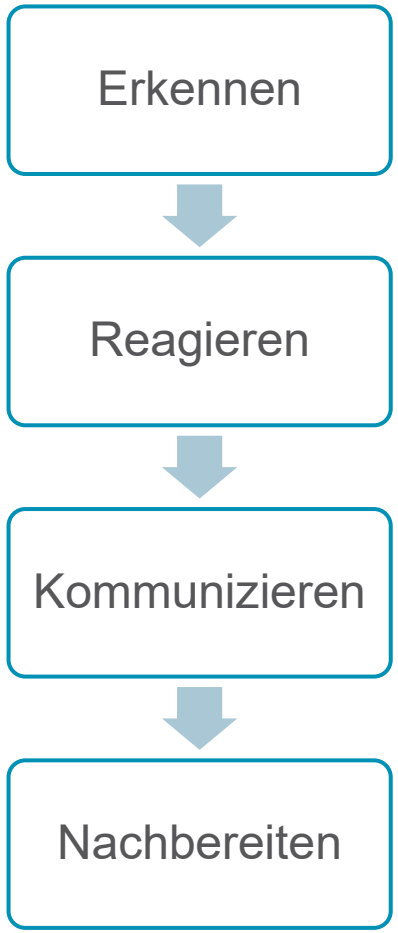
Reaktion:

8. Absender im Zweifel anrufen (nicht über E-Mail)
9. E-Mails sofort löschen
10. Meldung des Vorfalls

Schutz:

11. Backups anlegen
12. Betriebssysteme Patchen und Virenschutz aktuell halten
13. Internet-Adressen ggf. manuell eingeben

Reaktion auf Sicherheitsvorfälle - Incident Management



Sofortmaßnahmen:

- Angriff erkennen & bewerten
- Incident Response Team aktivieren
- Systeme isolieren
- Beweissicherung

Rollen & Verantwortlichkeiten:

- Klare Aufgabenverteilung
- Zusammenarbeit mit Datenschutz & Behörden

Meldewege & Kommunikation:

- Interne & externe Meldung
- Transparente Kommunikation

Nachbereitung:

- Ursachenanalyse
- Maßnahmen ableiten
- Dokumentation

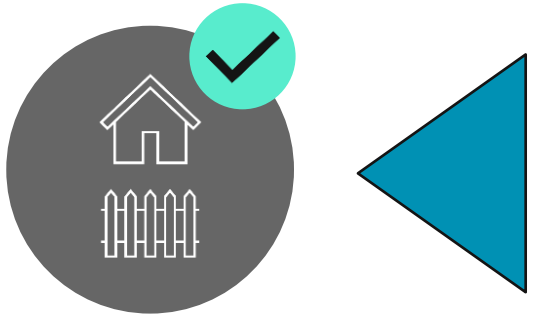
Prävention -
Systeme zur Angriffserkennung (SOC, SOCaaS)

- Zentrale Überwachung und Analyse aller sicherheitsrelevanten Ereignisse im Unternehmen
- Kombination aus Technik (Sensoren, Monitoring, Automatisierung) und Expertenwissen (Security-Analysten)
- Ziel: Angriffe frühzeitig erkennen, analysieren und Gegenmaßnahmen einleiten

- Kernfunktionen:
  - 24/7 Überwachung von Systemen, Netzwerken und Anwendungen
  - Anomalie- und Angriffserkennung durch Korrelation von Logdaten und Events
  - Integration bestehender Systeme (Firewalls, Virenschutz, Cloud, Endpoints)
  - Schnelle Reaktion auf Vorfälle (Incident Response)

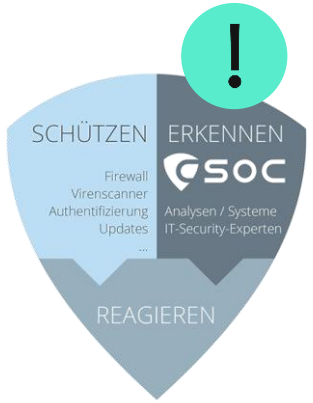
SOC/ SIEM > System zur Angriffserkennung

Grundlegende Eckpfeiler der Cyber Sicherheit



Schutz

- Technische Sicherheit, z.B. Endpoint-Lösungen, Firewalls, Schwachstellenscanner etc.
- Organisatorische Sicherheit, z.B. ISMS, Richtlinien, etc.
- Sicherheitsbewusstsein, z.B. Awareness Maßnahmen Mitarbeiter, etc.



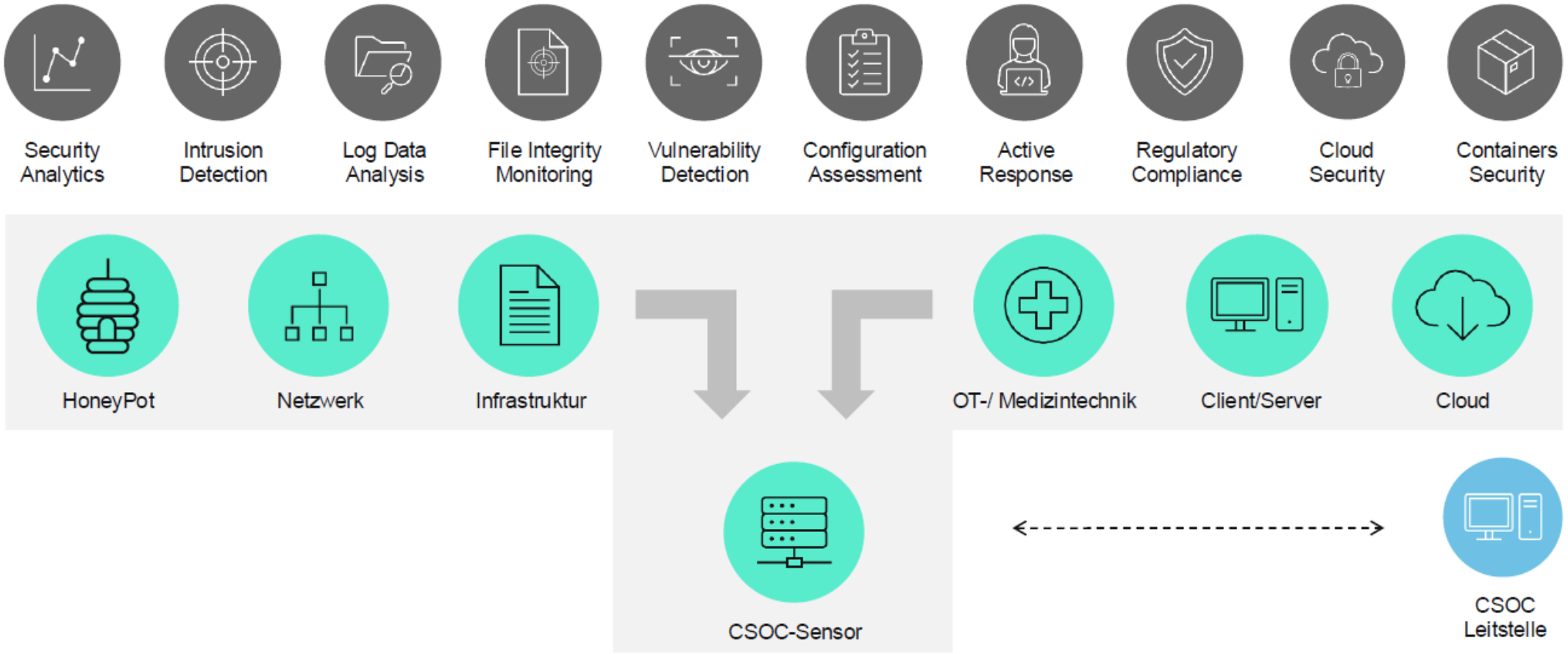
Erkennung

- Frühzeitige Erkennung von Schwachstellen, veraltete Software, Cyberangriffen, etc.

Reaktion

- Einleitung von Gegenmaßnahmen bei Angriffen
- Behebung von Schwachstellen
- (Durchführung von forensischen Analysen)

SOC - Eventkanäle



Reaktion auf Sicherheitsvorfälle - Business Continuity Management

- Minimierung von Auswirkungen, Ausfallzeiten und wirtschaftlichen Schäden
- Ziel: Sicherstellung der Geschäftsfähigkeit nach IT-Sicherheitsvorfällen

- Kernmaßnahmen:
  - Identifikation kritischer Geschäftsprozesse und IT-Systeme
  - Analyse und Bewertung der Auswirkungen von Störungen im Rahmen einer Business Impact Analyse (BIA)
  - Entwicklung und regelmäßige Überprüfung von Notfall- und Wiederanlaufplänen
  - Regelmäßige Backups und deren Wiederherstellung testen
  - Definition von Verantwortlichkeiten und Kommunikationswegen im Krisenfall

Vielen Dank für Ihre Aufmerksamkeit!

CLA Global

INDEPENDENT NETWORK MEMBER

dhpg

Wir beraten
Sie persönlich

CLA Global

INDEPENDENT NETWORK MEMBER

Ihr persönlicher Kontakt

Markus Müller
Geschäftsführer
CISA
CDPSE

dhpg
Erna-Scheffler-Straße 3
51103 Köln
T +49 221 292667 01
F +49 221 33636 36
E markus.mueller@dhpg.de

Kathrin Tjarks
Director
IT Audit & Digital

dhpg
August-Bebel-Allee 1
28329 Bremen
T +49 421 2388 162
F +49 421 2388 330
E kathrin.tjarks@dhpg.de

Felicitas Kellermann
Senior Manager
ISMS Auditor (TÜV)
IT Auditor IDW

dhpg
Hasenbergsteige 14
70178 Stuttgart
T +49 221 29266 714
F +49 221 33636 36
E felicitas.kellermann@dhpg.de

Haftungsausschluss

Dieses Handout wurde ausschließlich zur Präsentationsbegleitung erstellt.
Trotz größter Sorgfalt können wir keine Haftung für den Inhalt übernehmen.
Insbesondere kann es die persönliche Beratung nicht ersetzen.